네트워크를 통한 시스템 침입에 대한 고찰 II

조현호, 박영호, 이경헌
부경대학교 전자계산학과

A Study on Computer System Intrusion through Network II

Hyun-Ho Cho, Young-Ho Park, Kyung-Hyun Rhee
Dept. of Computer Science, PuKyong Nat'l University

요 약

본 논문에서는 최근 네트웍을 통해 실질적인 관리자 권한을 획득할 수 있는 공격기법을 살펴보고 그에 따른 대처 방안을 모색한다. 또한 Yahoo, CNN뿐만 아니라 최근 정부 및 교육기관 등에까지 막심한 피해를 입히고 있는 서비스 거부 공격(Denial of Service Attack) 각각의 공격 원리와 방어 방안을 고려하고, 악의적인 서버가 침입차단시스템을 회피하여 원격지의 클라이언트와 데이터를 송·수신할 수 있는 최근의 공격 기법을 소개한다.

1. 서론

현대사회는 정보기반 사회라고 일컬어도 과언이 아닐 정도로 정보는 중요시 되고 있다. 또한 컴퓨터 및 통신의 발달로 인해 이런 중요한 정보들이 엄청난 양으로 처리, 보관, 전송되고 있으며, 또한 고급정보의 전송 역시 증가하고 있다. 이와 같이 정보가 밀집화되고, 통신망 이용이 증가함에 따라 전문가적인 공격자뿐만 아니라 단순 호기심을 지닌 공격자에 이르기까지 시스템의 취약점을 악용하고, 인터넷 상에 공개된 툴 및 소스를 이용한 공격 역시 증가하고 있는 추세이다. 이런 추세의 배경에는 정부 및 교육기관, 그리고 회사 등 모든 사회구성요소에서 컴퓨터와 네트웍 기술을 급속하게 채용을 함에 따라 인터넷과 그에 따른 전자상거래가 활성화되어 더욱 복잡한 구조를 띄게 되어, 그 기술들에 내포된 잠재적인 취약점들이 점차 증가하였다는 것과, 또한 사회전반에 걸친 정보보호에 대한 의식의 결여 등이 있다.

공격자들은 날로 조직화되어가고 있으며, 그들이 사용하는 툴들은 취약점을 찾기 위해 소스 코드를 분석할 필요 없을 정도로 정교화되고 있으며, 또한 초보자도 사용할 수 있을 용이성과 대규모 공격을 지원하고 있는 실정이며, 그에 반해 인터넷 환경은 공격에 대한 추적(trace)을 하기가 쉽지 않아 현재 공격에 대한 효율적인 대응을 하기가 어렵다[2].

[8]에서 네트워크를 통한 시스템 침입 시나리오를 설정하고 모든 시스템 공격 기법의 시작이 되는 정보수집단계에서의 여러 방법을 논의하고 그에 대한 대책을 마련하였다. 본 논문에서는 정보수집단계 이후의 실제 침입에 사용되는 공격 기법 및 서비스 거부 공격(Denial of Service Attack)에 대해 초점을 맞추어 살펴보고 그에 대한 대응 방안을 모색한다. 본 논문의 순서는 2절에 버퍼 오버플로우 공격(Buffer Overflow Attack) 기법과 서비스 거부 공격들, 그리고 최근 기법인 ICMP Tunneling 기법에 대해 기술하고, 3절에서는 각 공격 기법들에 대한 대응 방법을 모색하며, 마지막으로 4절에서는 결론을 유도하고 향후 연구과제에 대하여 기술한다.

2. 공격 기법

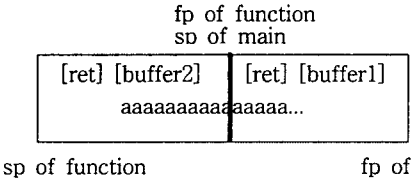
정보수집단계 이후의 실제 침입에 사용되는 공격기법 중 CERTCC-KR[3]에서 분석한 보고서에 의거하여 가장 많이 공격에 사용되는 버퍼 오버플로우 공격 기법과 날로 심각해져만 가는 서비스 거부 공격의 여러 기법들을 살펴본다. 또한 백도어(backdoor)와 같은 악의적인 서버가 침입탐지시스템을 통해 클라이

언트와 통신을 할 수 있는 최근 공격 기법인 ICMP Tunneling 공격 기법을 소개한다.

2.1 Buffer Overflow Attack

1996년 Bugtraq mailing list 운영자, AlephOne 이 Phrack Magazine 49호 "Smashing The Stack For Fun And Profit"[4]이라는 Article을 저술, 발표함으로써 이에 대한 세부적인 기술이 공개되었다. 버퍼 오버플로우 조건(buffer overflow condition)은 사용자 또는 프로세스가 원래 할당된 버퍼의 크기보다 더 많은 데이터를 저장함으로써 발생되는 것이다. 즉 데이터를 입력받을 때 한계값 검사(boundary check)를 하지 않음으로 해서 버퍼 오버플로우 조건을 이용하여 공격자의 임의의 일을 수행하는 공격하는 기법이다.

<그림 1>은 버퍼 오버플로우 조건이 발생했을 경우의 스택을 예시하고 있다. 이 경우는 buffer2의 크기보다 많은 데이터 'a'를 buffer2에 저장할 경우 오버플로우가 발생하여 다른 함수(function)의 ret영역, 즉 반환 주소(return address)를 저장하고 있는 부분을 덮어쓰고 있다.



<그림 1>

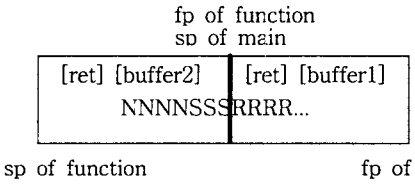
이러한 원리를 이용하여 ret를 조작한 정보로 덮어씀으로써 공격자가 원하는 임의의 일을 수행할 수 있게 된다. 즉, 위의 'a'대신에 공격자가 실행하고자 하는 프로그램의 주소로 바꾸어 넣는 것이다.

공격자는 보통 관리자 권한을 획득하려 할 것이기 때문에 이에 해당하는 루트 쉘(root shell)을 실행하려 할 것이다. 다음에 보이는 것은 Linux X86 system의 쉘 코드(shell code)이다.

"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd\x80\xe8\xdc\xff\xff\xff/bin/sh"

이 쉘 코드는 seed code 또는 Egg라고 하기도 하며, 운영체제에 따라 차이가 있는데, ret에서 이 코드를 가리키도록 함으로써 root shell을 실행시키게 된다.

<그림 2>에서와 같이, 버퍼 오버플로우 시킬 데이



N(N OPeration) : null 연산을 수행. 단지 지연의 목적으로 사용(0x90)
S(Shell code) : root shell의 assembly code
R(Return address) : N의 주소 값

<그림 2>

터를 입력하게 되면 버퍼 오버플로우 조건이 발생하고, 이 프로그램이 종료할 때 ret를 참조하게 되어 공격자가 의도한 루트 쉘을 실행되게 된다. NOP(N) 코드를 사용하는 이유는 정확한 버퍼의 크기를 알 수 없고, 또한 반환 주소를 정확히 쉘 코드로 지정할 수 없기 때문에 공격의 성공률을 높이기 위해 삽입하는 것이다.

2.2. Denial of Service Attack

서비스 거부 공격은 대상 서버 또는 시스템이 서비스를 하지 못하도록 하는 공격으로 네트웍의 대역폭(bandwidth)를 다 소모하게 하게 하거나 또는 대상 시스템의 자원(resource)을 소모하게 하여 속도를 저하시키고, 또는 공격자가 조작한 패킷을 대상 시스템으로 전송하여 예기치 못한 상황을 일으키게 하는 공격기법이다.

여러 서비스 거부 공격 기법들은 아래의 유형으로 나뉘어질 수 있다[5].

- Bandwidth Consumption
- Resource Starvation
- Programming Flaw

Bandwidth Consumption 유형은 특정 네트웍에서 허용하는 대역폭을 다 소모하게 하여 결국 그 네트웍상의 시스템이 서비스를 못하도록 한다. 예를 들어, 대상시스템의 네트웍 대역폭이 T1급인 1.544Mbps라고 할 때, 공격자가 그 허용범위보다 큰 트래픽을 전송함으로써 대상시스템이 서비스를 못하게 하는 유형이다. 그리고 Resource Starvation 유형은 bandwidth consumption 유형과 비슷하나, 네트웍 자원이 아닌 대상 시스템의 자원(CPU, Memory등)을 소모하게 하

는 유형이다. 마지막으로 Programming Flaw 유형은 대상시스템 상에서 동작하는 운영체제, Application등의 프로그래밍 오류에 대한 공격으로 서비스를 거부하게 하는 유형이다. 즉 프로그래밍시에 명시하지 않은 옵션(option)을 가진 패킷을 수신하게 하거나, 또는 버퍼 오버플로우 조건을 일으켜 예외상황을 발생시킴으로서 DoS 공격을 시도하는 유형을 말한다.

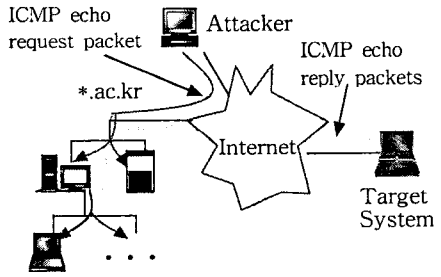
본 절에서는 여러 기법들 중 많이 공격에 이용되고 있는 몇 가지 기법들을 살펴본다.

2.2.1 SYN Flooding

SYN Flooding 기법은 대상 시스템에 SYN 패킷만을 대량으로 전송하여 TCP 서비스 연결(connection)을 거부하도록 하는 기법이다. 즉 공격자가 대상 시스템에 SYN 패킷을 전송하면 대상시스템은 three-way handshake 절차에 의해 SYN/ACK 패킷을 전송하고 SYN_RCVD 상태에서 ACK 패킷을 수신할 때까지 대기하게 된다. 이러한 half-open 연결만을 시도하기 위해 공격자는 계속적으로 SYN 패킷을 전송하여 결국 대상시스템의 대기 큐(listening queue)의 공간을 채워 TCP 서비스 연결을 맺지 못하도록 하는 기법이다.

2.2.2 Smurf

이 공격은 네트워크에 엄청난 트래픽을 유발시키는 공격 기법으로 ICMP 패킷을 사용하며 ping 프로그램을 조작하여 이 DoS 공격을 실행할 수 있다.



<그림 3>

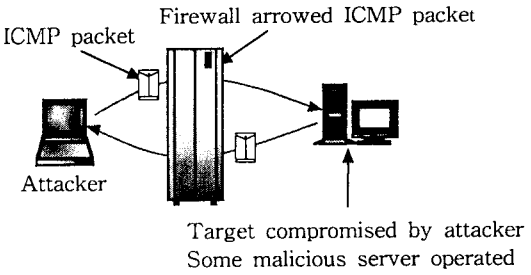
공격 원리는 <그림 3>에서 보이는 것처럼 공격자가 ICMP echo request 패킷을 생성하는데, 이 패킷의 근원지 IP 주소(source IP address)를 대상 시스템의 IP 주소로 설정된다. 그 후 대단위 네트워크로 방송(broadcast)하면 이 네트워크의 모든 하위 시스템들이 이 ICMP echo request 패킷에 대한 응답으로서 ICMP echo reply 패킷을 대상 시스템으로 전송함으로 인해 대량의 패킷들이 집중하게 되어 엄청난 트래픽을 발생시켜 결국 서비스를 거부하게 한다.

2.2.3 Teardrop

네트워크 상에서 전송할 데이터의 크기가 클 경우 MTU단위로 분할하여 전송하게 되고, 수신측은 패킷의 헤더의 정보로 분할된 패킷들을 재조립하게 된다. Teardrop 기법은 두 UDP 패킷을 가지고 이러한 사실을 이용하여 공격을 하게 된다. 즉 전송할 두 번째 패킷의 헤더 정보(offset)를 조작하여 수신측의 재조립과정에서 버퍼 오버플로우 조건을 발생시켜 시스템을 정지시키거나, 또는 첫 번째 패킷의 헤더부분에 덮어써 불완전한 패킷을 생성하게 함으로써 커널의 메모리를 소모하게 만들어 결국 전체 시스템의 속도를 저하시키도록 한다.

2.3 ICMP Tunneling

대부분의 침입탐지시스템들이 ICMP ECHO REQUEST, ICMP ECHO REPLY 패킷들을 허용한다는 사실을 이용하는 기술이다[6].



<그림 4>

이 공격 기법은 대상 시스템이 공격자에 의해 이미 해킹 당하였으며, 악의적인 서버(backdoor server)가 동작 중이라는 것을 가정한다. 즉, 침입탐지시스템에 의해 보호되는 대상 시스템에서 동작중인 악의적인 서버와 공격자 시스템의 클라이언트는 침입탐지시스템을 통하여 데이터를 송·수신하기 위해 침입탐지시스템이 ICMP 패킷을 허용한다는 점을 이용하여 ICMP 패킷의 헤더부분에 데이터를 삽입, 송·수신한다. 이 기법은 phrack article에 먼저 소개되었으며, 이미 lokid라는 프로그램이 개발되었으며, 이론상으로는 ICMP 패킷뿐만 아니라 다른 protocol에도 적용이 가능하다. 또한, 검출(detection)이 어렵기 때문에 숨겨진 채널(covert channel)이라고도 한다.

3. 대응 방안

버퍼 오버플로우 공격에 대한 대응 방안으로서는 앞서 언급하였듯이, 네트웍 상에서 사용자 또는 프로그램으로부터 입력 데이터를 수신할 때 입력 값에 대한 한계값 검사를 하지 않음으로 인해 가능한 공격이기 때문에, 프로그래밍 단계에서 Security에 대한 의식을 가지고 프로그래밍을 해야한다. 즉, 데이터를 수신할 때 반드시 한계값 검사를 수행하여야 하며, 그러기 위해 fgets(), strncpy()와 같은 안전한 루틴(routine)들을 사용해야한다. 또한 스택 상에서 실행될 수 없도록 no-stack execution을 설정할 수가 있는데, Linux 2.0.x kernel의 경우 이 설정을 할 수 있는 patch가 존재하며, 또한 patch 후 /etc/system 파일에서 다음과 같이 설정한다.

```
set noexec_user_stack=1
```

그리고 버퍼 오버플로우의 공격 대상이 되는 프로그램이 SUID 루트를 가지는 프로그램이므로, SUID 루트 프로그램의 사용을 최소화하는 것도 한 대응 방안이 될 수 있다.

서비스 거부 공격중 SYN Flooding 공격을 당했을 때 Linux 시스템일 경우 netstat command를 사용하여 많은 연결이 SYN_RCVD 상태로 존재하고 있는 것을 볼 수 있다. 대응 방안으로서는 연결 큐의 크기를 증가시키고, 연결 설정의 time period를 감소시키는 방법이 있으나 다소 공격의 영향만 감소시킬 뿐 완전한 대처방안은 될 수 없다. 그리고 최근 들어 공공기관 및 대학 등을 대상으로 유행하고 있는 Smuf 공격에 대해 대상시스템의 측면에서 대처할 수 있는 방안은 없다. 단지 이 공격을 가능하게 하는 중간 단계의 시스템으로서 이런 directed-broadcast에 대한 응답을 하지 않도록 설정이 가능하다. 먼저 라우터(router)에서 directed broadcast 기능을 사용하지 못하게 할 수 있는데 Cisco router의 경우 no ip directed-broadcast command를 사용하여 설정이 가능하고, 그리고 Solaris 2.6, 2.51, 2.5, 2.4, 2.3 시스템에서는 /etc/rc2.d/S69inet에서 다음과 같이 설정할 수 있다.

```
ndd -set /dev/ip ip_respond_to_echo_broadcast 0
```

Teardrop에 대한 대응 방안으로서는 이에 대해 각 운영체제마다 그 벤더(vendor)의해 공개된 patch를 시스템에 적용하는 것이다. NT system의 경우 MS사에 의해서 Teardrop2-fix patch가 있으므로 적용하면 해결된다.

ICMP Tunneling 공격기법에 대한 대응 방안으로서는 무엇보다 이러한 악의적인 서버가 침입하지 않도록 해야하며, 또한 현존하는 악의적 서버가 언제 이 ICMP Tunneling 기법을 이용하는 변종으로 발전할지 모르기 때문에, Anti-virus software로 detect하여 제거해야함은 물론, 침입탐지시스템에서의 ACL(Access Control List)을 이용한 필터링보다 프락시 기반의 침입탐지시스템에서의 컨텐츠 필터링이 수행되어져야만 한다.

5. 결론

본 논문에서는 최근에 가장 많이 응용되고 있는 버퍼 오버플로우 공격 기법의 원리를 살펴보았으며, 또한 전 세계적으로 막대한 시간 및 경제적인 피해가 속출하고 있는 서비스 거부 공격의 몇 가지 기법들, 그리고 악의적 서버가 침입탐지시스템을 회피하여 클라이언트와 데이터를 송·수신하는 최근의 기법에 대하여 살펴보았으며, 각각에 대한 대응 방안을 모색해 보았다.

요즘 security software로서 많은 침입탐지시스템과 침입탐지시스템(Intrusion Detection System)제품들이 출시되고 있다. 대부분의 경우 ACL 기반의 침입탐지시스템이고 또한 IDS 역시 공격자의 정보수집단계에서의 검출에 불과한 실정이다. 따라서 본 논문에서 논의하였던 공격원리와 대책을 보완, 발전시켜 침입탐지시스템의 정책(policy)에 적용, 컨텐츠 필터링을 수행한다든지, 또는 침입탐지시스템의 DB에 적용한다면 효과적인 방어를 수행할 수 있을 것이다.

[참고문헌]

[1] S. McClure, J. Scambray, G. Kurtz, "Hacking Exposed", Osborne/McGraw-Hill, 1999.
[2] http://www.cert.org/present/cert-overview-trends/sld001.htm
[3] http://www.certcc.or.kr
[4] http://phrack.infonexus.com/
[5] ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40
[6] http://oliver.efri.hr/~crv/security/bugs/
[7] ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/hotfixes-postsp3/teardrop2-fix/
[8] 신원, 이경현, "네트워크를 통한 시스템 침입에 대

한 고찰", '2000 한국멀티미디어학회 춘계학술발표
논문집, pp.86-89, 2000.